The

South Carolina Department of Consumer Affairs

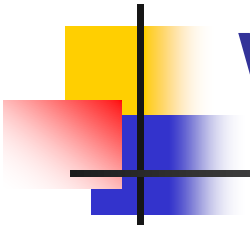
SCAMS AND SCHEMES AND IDENTITY THEFT

About the South Carolina Department of Consumer Affairs

- Licenses several types of businesses – such as pawn shops, mortgage brokers, consumer credit counselors, physical fitness facilities
- Handles complaints for family, household or personal goods or services

We will talk about:

- Popular Scams
- Identity Theft



What you will learn:

- Measure twice and cut once!
- If it seems too good to be true, it probably is!
- There is no such thing as a free lunch!

Nigerian Scam

Claiming to be Nigerian officials, businesspeople or the surviving spouses of former government officials, con artists offer to transfer millions of dollars into a bank account in exchange for a small fee. If the consumer responds to the initial offer, he may receive "official looking" documents. Typically, he is then asked to provide blank letterhead and his bank account numbers, as well as some money to cover transaction and transfer costs and attorney's fees.

Variations

- You receive notice that a relative in a foreign country died and you get the estate, if you first send money to cover taxes and other fees.
- Someone needs to cash payroll checks but doesn’t have access to a checking account. You are to cash the check, keep a small portion and send the remainder to them.

International Lotteries

Scam operators often based in Canada — are using the telephone and direct mail to entice U.S. consumers to buy chances in high-stakes foreign lotteries from as far away as Australia and Europe. These lottery solicitations **violate U.S. law**, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

If you play a foreign lottery-through the mail or over the telephone-you're violating federal law. There are no secret systems for winning foreign lotteries. Your chances of winning more than the cost of your tickets are slim to none. If you purchase one foreign lottery ticket, expect many more bogus offers for lottery or investment "opportunities." Keep your credit card and bank account numbers to yourself.

Remember:

- NEVER allow your accounts to be used for money laundering!
- NEVER give your financial account information to strangers!
- Even real looking cashier's checks can be phony!
- When the checks bounces, YOU OWE THE MONEY BACK TO THE BANK!

Identity Theft:

- How ID theft happens
- How to avoid it
- What to do if it happens to you

How does it happen? Thieves get info in a variety of ways:

- From you – when they ask!
- Lost or stolen wallets or receipts
- Preapproved offers
- Dishonest bank,car dealer or credit company employees
- Bogus bank/IRS forms returned to them by unsuspecting consumers
- Registration information
- Over the Internet

Minimize your risk

Shred unnecessary documents and old receipts, files, and records.

Check your credit report at least once a year.

Don’t give your information to unfamiliar people or businesses.

Ask people why they need the information? What will they do with it? How will they protect it? With whom will they share it?

Protect Your Mail and Your Trash

Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox.

Stop an identity thief who may pick through your trash or recycling bins to get your personal information: tear or shred information.

And A Few More Tips...

Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time.

Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information.

Opt Out When Possible

More organizations are offering people choices about how their personal information is used including an opt-out choice that limits the information shared with others or used for promotional purposes.

Pre-screened Credit Offers

If you receive pre-screened credit card offers in the mail (based on your credit data), tear them up after you decide you don't want to accept the offer.

To opt out of receiving pre-screened credit card offers, call: 1-888-5-OPTOUT (1-888-567- 8688).

Telemarketing

The federal government has created the National Do Not Call Registry — the free, easy way to reduce the telemarketing calls you get at home. To register visit www.donotcall.gov, or call 1-888-382-1222 from the phone you want to register.

Mail

The Direct Marketing Association's (DMA) Mail Preference Service lets you "opt- out" of receiving direct mail marketing from many national companies for five years.

E-Mail

The DMA also has an EMail Preference Service to help you reduce unsolicited commercial emails. To “opt-out” of receiving unsolicited commercial email, use DMA’s online form at www.dmaconsumers.org/offemaillist.html

Social Security Numbers

Your employer and financial institution need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check. **You don't have to give a business your SSN just because they ask for it.** ASK QUESTIONS!!

A business may not provide the service or benefit you're seeking if you don't provide your SSN. Remember — THE DECISION IS YOURS.

Computer Safety

Do not download files sent to you by strangers or click on hyperlinks from people you don't know.

Use a firewall program to stop uninvited guests from accessing your computer.

Use a secure browser — software that encrypts or scrambles information you send over the Internet. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

Credit Freeze

- South Carolina law (§37-20-110 *et.seq.*) allows you to have your credit file "frozen" at no cost
- You must contact each credit reporting agency separately
- You will be given a PIN for thawing your report. Thawing takes from 15 minutes to 3 days
- You can freeze and thaw as many times as needed

ID Theft “Insurance”

- Several companies offer ID theft insurance or protection
- Consumer should be very wary of these contracts
- Consumer should read the policy or contract carefully to determine what is (and is not) covered

What to do if your identity is stolen

If you suspect that your personal information has been misappropriated to commit fraud or theft, take action immediately.

There are four basic actions you need to take appropriate in almost every case.

First Step if your identity is stolen: credit reporting agencies

- Call the toll-free fraud number of any one of the three major credit bureaus to place a fraud alert on your credit report.

- As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

Second Step if your identity is stolen: close accounts

- Close any accounts that have been tampered with or opened fraudulently.
- If you're closing existing accounts and opening new ones, use new Personal Identification Numbers (PINs) and passwords.
- If there are fraudulent charges or debits, ask the company for the form to file to dispute the transactions.

Third Step if your identity is stolen: report to police

- **File a report with your local police or the police in the community where the identity theft took place.**

  Keep a copy of the report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number.

Fourth Step if your identity is stolen: Federal Trade Commission

- **File a complaint with the FTC.**

- By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them. The FTC enters the information you provide into a secure database.

Resources

- www.scconsumer.gov
- www.ftc.gov/consumer
- www.bankrate.com
- www.moneycentral.msn.com